IA-00013

Concept of Operations

for a

Corporate Information Protection Program

Lee Sutterfield
Information Warfare Strategic Planner
Air Force Information Warfare Center
250 Hall Blvd Suite 347
San Antonio, TX 78243-7063
(210)509-4626
lsutt@texas.net

SUMMARY

The Corporate Information Protection Program (CIPP) described in this paper is an attempt to move concepts developed within the Air Force C4 Systems Security Assessment Program to a form that may prove useful for all government agencies and commercial organizations. The Air Force and other Department of Defense organizations are rapidly adopting this program with increasing success. The focus of the Air Force program is to exercise an operational capability to continuously measure security posture and predict, deter, detect, intercept, isolate/contain, and recover from attacks against information systems. Lessons learned and data collected in this process are fed to the planning and acquisition processes for the upgrade of information systems technologies and corporate protection capabilities. It's based on the application of Statistical Process Control theory and practice and the view of computer and network security as an operational issue as opposed to just a regulatory issue. Today's Information Technology managers are faced with a rapidly evolving technology based on open systems and extensive connectivity. With this new capability comes risks of intrusions and information compromise. Those who are not yet convinced of the risks need only wait. The risk will become clear soon enough. For those who are convinced that action is needed, what's the answer? Firewalls, encryption, intrusion detection tools, good system administration, TCP wrappers, etc? IT manager's are bombarded daily with the latest tools that will fix the problem and let them sleep better at night. However, many of these tools are of little use unless applied in some systematic way. In fact, corporate IT environments are often so poorly configured for security control that use of these tools usually does more harm than good. What is needed more than the tools is a process and operational capability to identify problems and potential solutions and systematically drive efforts to incrementally improve security pbsture. The CIPP concept of operations offers the framework from which an effective corporate capability may be built.

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00001995	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Concept of Operations for a Corporate Information Protection Program	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Air Force Information Warfare Center 250 Hall Blvd Suite 347 San Antonio, TX 78243-7063	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 9	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 9/1/95	**3. REPORT TYPE AND DATES COVERED** Periodical

4. TITLE AND SUBTITLE
Concept of Operations for a Corporate Information Protection Program

5. FUNDING NUMBERS

6. AUTHOR(S)
Lee Sutterfield

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Corporate Information Protection Program (CIPP) described in this paper is an attempt to move concepts developed within the Air Force C4 Systems Security Assessment Program to a form that may prove useful for all government agencies and commercial organizations.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** None

BACKGROUND

The DoD's efforts in the late sixties and seventies to develop a robust computer communications network capability has evolved into today's Internet. Amid all the discussion of the utility of the Internet for business and government there seems to be growing consensus on only one issue-security is a problem. The ARPANET, from which the Internet has grown, was built to survive large scale war in the physical domain. Large scale, unauthorized activity in the information domain was not considered a problem since the early environment in which the technology was developed was a small, fairly considerate community. However, today's level of unauthorized and increasingly malicious activity occurring within corporate and worldwide intemets threatens the value of intemetworking.

In the past, the costs of internetworking were based on the costs of planning, purchasing hardware, software and transmission capacity, system administration, etc. Internetworking costs did not include security until recently. The cost of security can appear to be high at first and so it soon becomes an area to cut until a major event happens and resulting costs threaten corporate profitability and/or market position. Though the costs of poor security posture can be high, it is the lack of predictability that can be more devastating. How does one plan for the loss of trade secrets, alteration of key operational data, fraud, etc? If contingency plans for such catastrophes were prepared honestly and based on real data quantifying today's corporate security posture, most IT managers would never sleep.

The key to success for the computer and network security problem is not technology. It's diligence. What is needed is a systematic effort to characterize and quantify security posture in operational terms, seize control of it just as we do any other operational process, and integrate the information protection processes into everyday corporate operations. Only through this systematic approach does one have hope of relating the cost of security to the cost of goods sold. Though the Air Force doesn't sell goods, recent cuts have clearly focused attention on the cost of goods used, so the computer and network security program within the Air Force has had to face repeated assessments of its cost-effectiveness from both within and without. This scrutiny has led to a focus on the development of capabilities that have wide applicability throughout corporate Air Force. What has evolved is a fairly efficient use of existing technologies and resources to seize control of security posture. So, just as the ARPANET has evolved into a capability that offers commercial value, so the Air Force computer and network security program has evolved into a form that may offer commercial value.

Much has been written and reported in the news media regarding the vulnerabilities of computers and the exploitation of those vulnerabilities over the growing number of interconnected computer networks. For those not yet convinced of the security problems associated with today's connectivity you'll find this paper confusing. I make no attempt to convince. If however, your looking for a practical approach to protecting corporate information systems, read on.

COMPUTER SECURITY AND STATISTICAL PROCESS CONTROL

The Air Force began the application of Statistical Process Control theory to the problem of Infosec in late 1990. The effort is driven by the realization that the effectiveness of our Infosec program over the past 15 years has been inadequate. Despite considerable efforts to clearly define policy and guidance, write regulations, conduct education and awareness, incorporate security requirements into the acquisition cycle, and inspect field units for compliance, the security posture of Air Force information systems has not improved. In fact, with the increase in connectivity between systems and the rapid turnover in technologies it can be argued that security posture is worse now than it has ever been. When all is said and done, if our security program is working, it should be more difficult to break into and exploit Air Force systems. That hasn't been the case in the past, but we've recently begun to see measurable improvements. The reason is we've committed to a systematic, institutionalized effort to characterize and quantify security posture in terms everyone understands and to implement continuous, incremental improvement in that security posture. We've shown that the use of Statistical Process Control methods is the most effective way to manage risk in this complex environment.

A full discussion of the philosophical, technical and operational implications of the application of Statistical Process Control (SPC) theory and Total Quality Management principles to this problem is beyond the scope of this paper. However, in general terms, we've built capabilities to address a systematic approach to the Plan-Do-Check-Act cycle used to guide the implementation of SPC.

CORPORATE INFORMATION PROTECTION PROGRAM (CIPP)

The CIPP is an attempt to apply risk management principles to the problem as opposed to risk avoidance which has been the approach to information security in the past. The CIPP has four main purposes:

1. Characterize and quantify security posture in terms the customer understands.

2. Use the data collected in that process to drive the development or acquisition of countermeasures tools. Such decisions must be based on data, not intuition.

3. Drive the implementation of countermeasures in the field. We must have the ability to measure the effectiveness of countermeasures in operation, quantify the incremental improvement of security posture and determine the exact cost of each countermeasure.

4. Exercise the corporate ability to protect information systems. As in any endeavor, practice makes near perfect. Corporate bodies must practice protecting their systems as a matter of daily operations. "One must walk those digital hallways and rattle those binary knobs" if they want to "know" how well they're doing.

The structure of a central coordination team supporting distributed smaller teams in the field is essential for large communities. Managing security posture and risk within a large community with diverse missions and computer support structures requires clearly defined roles and responsibilities and a dynamic operational structure that can allow for the rapid, corporate-wide change of system configurations.

Thus, a large organization may need to establish midlevel "Enterprise Network Control Cells" to work directly with a Central Control Center. Wise use of existing system administrator and other IT resources will minimize the necessary investment. Mush can be done through changing processes, redefining roles/responsibilities and specialized training. Once the CIPP reaches full operational capability, the corporation will have the ability to predict and/or detect an attack, determine the operational and technical profile of attack, alert corporate detection and control systems, issue configuration and control requirements to mitigate the attack and implement those changes world-wide within a matter of hours. Before long they can become proactive through good planning based on CIPP data. This can all be done for much less than it might seem at first.

CIPP Concept of Operations

Figure 1 shows the structure of the CIPP. There are three main levels of activity. The CIPP Operations layer, which is essentially on-line services and activities; the CIPP Technical Support layer, which is a set of specially trained technical teams; and the Statistical Analysis and Reporting layer which uses the data collected by the first two layers for strategic reporting and planning purposes.

A CIPP may be implemented in many different ways but each of the functions outlined below must be addressed in some form. Various functions may prove cost-effective to do in-house and others may need to be outsourced to some degree. However, because the core function of Statistical Analysis and Reporting will provide inputs to the corporate strategic planning process, some m-house investment must be made here to fully integrate the CIPP into daily corporate operations.

The ultimate return on investment and effect on long-term corporate profitability must, of course, be decided from within. This requires some in-house investment in understanding the issues involved and the methods used. The CIPP should be based on the premise that security posture is quantifiable, the metrics used to characterize security posture should be meaningful from a business perspective and the methods for data collection and security posture improvement should leverage existing corporate investments.

The first two layers do two things. First, they provide specialized services and tools that help corporate resources manage security posture and take special protective actions when necessary. Second, they collect important data on security posture. Every action taken by these two layers should be leveraged to collect data that sheds light on the cost-effectiveness of the CIPP processes. The third layer analyzes the data collected by the first two layers and provides the results to senior management. The third layer also drives the metrics from a statistical and financial perspective to continually improve the CIPP processes and keep costs down. Let's examine each function in more detail.

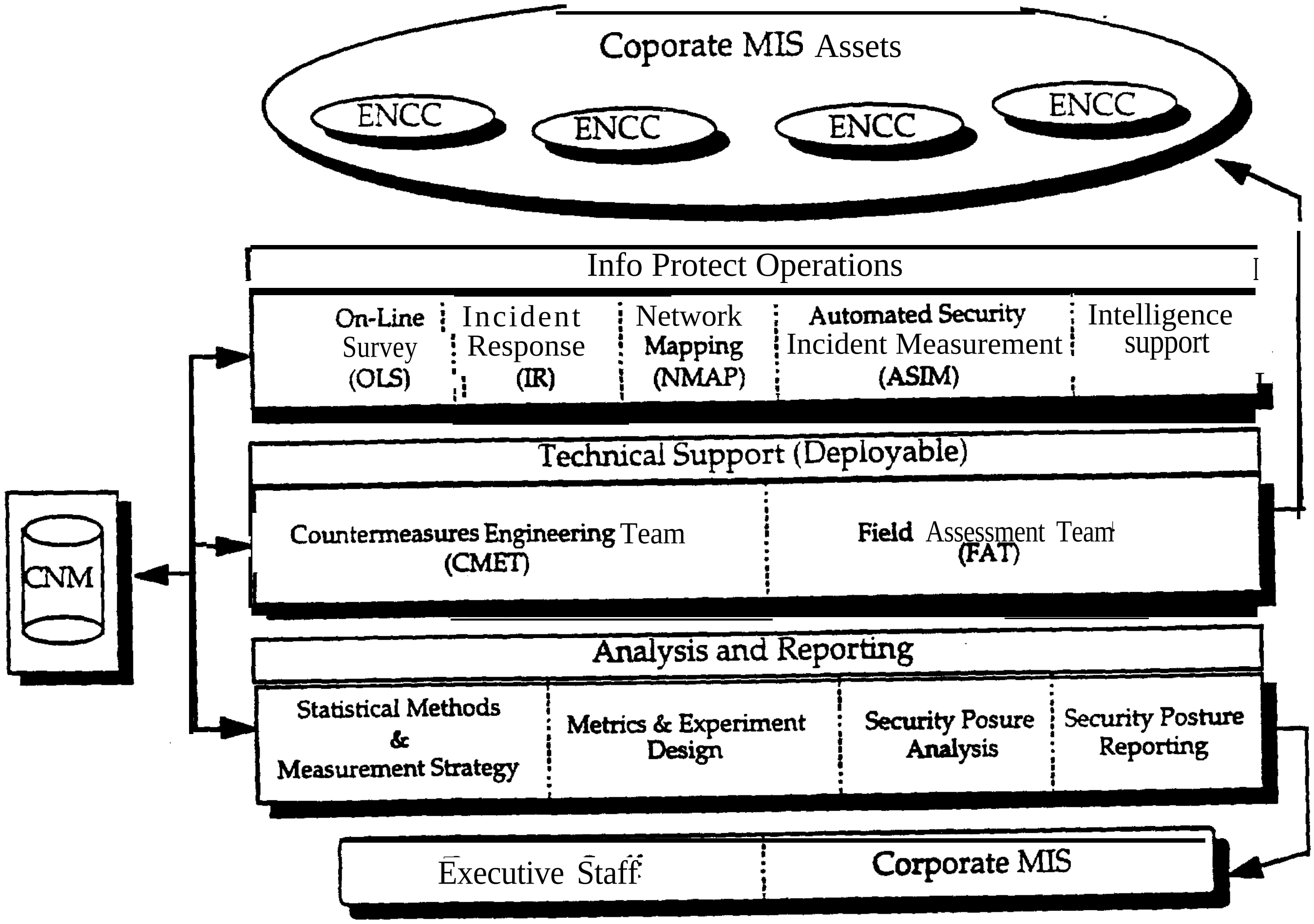
Coporate MIS Assets
ENCC
ENCC
ENCC
ENCC
Info Protect Operations
On-Line Survey (OLS)
Incident Response (IR)
Network Mapping (NMAP)
Automated Security Incident Measurement (ASIM)
Intelligence support
Technical Support (Deployable)
Countermeasures Engineering Team (CMET)
Field Assessment Team (FAT)
CNM
Analysis and Reporting
Statistical Methods & Measurement Strategy
Metrics & Experiment Design
Security Posure Analysis
Security Posture Reporting
Executive Staff
Corporate MIS

Figure 1. CIPP Concept of Operations.

CIPP OPERATIONS

On-Line Surveys (OLS).

The OLS Team should have the authority to attack any identifiable corporate computer and network system without notification and measure a given vulnerability state, the ability of the target to detect the attack, the ability to report that attack to the Incident Response Team (IRT), and the IRT's ability to provide a meaningful Recommended Course of Action (RCOA) back to the site under attack. The OLS function is really the front end of the CIPP effort to exercise corporate capabilities to protect information systems. Results from the Air Force effort have confirmed that though we've provided security guidance to the field over the years, that guidance hasn't been translated into effective protection practices at the system level.

Though we don't have time to describe them in this paper, we've characterized seven categories of attacks. Level 1 is the simplest and least disruptive and Level 7 is what we call full exploitation and control. Our current OLS activity is focused on the first three levels of attack. In general terms, we're concentrating on closing the "front doors" on as many systems as possible, as quickly as possible, Once we've reached an acceptable level of risk at this level, we'll move on to deeper levels of attack, again, covering as many systems as possible during the year. We've already shown small improvements in security posture and are confident that it will improve-considerably in the next year. Of most importance, we'll be able to quantify the level of improvement rather than guess at the level of improvement as we've done in the past.

The OLS function should not be just an exercise in showing how easy it is to break into systems. Recent efforts by some groups to grab the latest tools, such as SATAN, and run them against their systems have often led to a false sense of security. Breaking into a few systems is one thing, systematically measuring and improving security posture is another. OLS's must be used to educate system administrators and users of the consequences of poor security practices.

Incident Response Team (IRT)

When the field detects the OLS attacks, or real attacks, they report them to the IRT. The IRT's mission is to control all operational aspects of the CIPP, conduct and coordinate incident response, direct the building and management of the Network Map and coordinate the technical support provided to the criminal investigative community by CIPP resources if that becomes necessary. The IRT controls and coordinates the basic incident response process which has five steps: detection, reporting, technical assessment, isolation and containment, and recovery. The purpose of this process is to identify and mitigate the electronic activity directed against corporate systems.

This process does not attempt to identify the perpetrator of the attack. That's the role of the criminal investigative community. If the decision is made to open a criminal investigation, the IRT coordinates technical support for the investigative body if requested. The legal issues surrounding incident response are numerous, but many of these issues are much clearer today than a few years ago. Full support to criminal investigations can become costly if not managed properly. An IRT should conduct operational and cost analysis ahead of time before corporations run headlong into supporting criminal investigations. However, long-term returns for doing so, though difficult to quantify, usually justify such an effort.

Network Mapping (NMAP)

The Network Map (NMAP) function previously mentioned is a key element of the CIPP. A full description of a network map is beyond the scope of this paper. However, within the Air Force program efforts are underway to build the first comprehensive NMAP for management of security posture. Use of existing commercial network management software with some added functions will give us a first cut in the next year. Full NMAP tools will eventually be available commercially. It will eventually be a data base tied to a geographical map that provides all needed data to control security posture. The NMAP will contain information on hardware and software, connectivity, system administrator information, operational mission description, sensitivity data, criticality data, data descriptions, vulnerability status, etc. The NMAP capability will eventually lead to on-line accreditation for networked systems. Investment in this tool will prove invaluable for myriad IT issues beyond information protection.

Automated Security Incident Measurement (ASIM).

The ASIM capability is equivalent to "cyberspace radar". Its purpose is to detect attacks against systems and report those attacks in near real-time to the IRT and to the field units under attack. ASIM is the backbone of an effective CIPP. Diligence in cyberspace is possible only if it is automated. The intent should be to field intrusion detection and network monitoring software corporate wide. Under the ASIM capability, the output for a small subset of LAN's using the intrusion detection software is fed back to the CIPP Operations team. If an organized attack is targeted against a number of corporate systems, ASIM will pick up indicators quickly. The Air Force has already had strong results from its limited ASIM capability and is currently fielding the next generation.

Confusion abounds regarding the monitoring of computers and networks. Though the discussion is beyond the scope of this paper, the law and standard practices support a ***strong*** monitoring capability for security purposes for both government and commercial bodies. The sophistication of intrusion detection and system monitoring technologies is growing rapidly. The problem is that the user must be fairly skilled to interpret alarms and to take effective action. Nonetheless, a growing set of products and services are available on the commercial market to assist with this function if in-house expertise is too limited.

Intelligence Production Support.

The role of intelligence support in commercial information protection has never really been addressed. In simple terms, there is a great deal of information available regarding threat to information systems. Membership in security associations and subscription to some security publications can provide a wealth of information. Though it is usually hard to justify in-house resources for this function it shouldn't be overlooked.

CIPP TECHNICAL SUPPORT

The technical support layer has two levels of deployable teams. Each level has two purposes. First, they have specific technical services that they perform for customer organizations to help improve security posture. Second, while performing these services they collect data on security posture metrics for use by the Statistical Methods and Analysis Team for strategic planning.

Field Assessment Teams

The FATs perform specialized field support for security improvements and incident response. They should play a big role in technical training of system administrators. They learn to use the latest in tools and practices and package the operational capability for system administrators in the field. Though few corporate bodies can afford full time FATs, many are finding it very useful to outsource this support on occasion to help with fundamental corporate-wide security problems.

Countermeasure Envineerinv Team (CMET).

The CMET operates at the engineering level and validates new vulnerabilities, develops countermeasures and prototypes specialized protection tools to be used by the CIPP and field level personnel. The CMET is a specially selected team that has the skills to also seek out new vulnerabilities before others find them. Their mission is to keep their corporate owner technically ahead of potential adversaries. Again, this is a vital function that may seem too costly. However, a growing number of firms offer sound technical support such as described, and if it is integrated by a group that has the operational experience it can more than pay for itself.

STATISTICAL ANALYSIS and REPORTING

The Statistics Team analyzes the data collected by the operations and technical support layers, does strategic planning for Info Protect, provides the results to MIS and other executive staff, and manages the CIPP. Based on findings, they recommend initiatives for the development of tools, technologies, countermeasures, and upgrades to structures needed for operations, etc. They also interface with other agencies and national bodies for planning purposes. The management of the CIPP includes metrics development, experiment design, resource programming and planning, security posture analysis, security posture reporting, policy recommendations and strategic planning.

CONCLUSION

Today's IT manager is faced with a dynamic environment that if not managed properly can hurt productivity and profitability more than any other single factor. Security is a new variable in the management formula that has been ignored for many years, but that will not be the case in the future. Governments and industry throughout the world will increasingly see the need to control IT security posture. The CIPP Concept of Operations above has been shown to be cost effective for the Air Force. Time and appropriate implementation changes may prove it's cost-effectiveness for other government agencies and industry.